U.S. Department of State, Information Resource Management,

Office of Information Assurance, February 14, 2011

Security Dashboard
US Department of State

The Department of State continuously monitors and reports risk on its IT infrastructure. We have been quite successful and have been identified as a best practice for management reporting of infrastructure risk. One of the principal systems used in this worldwide endeavor is a custom developed application called iPost.

OpenNet is the Department of State's global network which serves 285 foreign posts and a multitude of domestic bureaus and locations. It consists of approximately 5,000 routers and switches, and more than 40,000 hosts. Overseas, almost all network and system administration is the responsibility of local staff. Although there is considerable centralization, administrative responsibility is somewhat dispersed. iPost allows local administrators to monitor security data within their scope of their responsibility and management statistics for reporting at the Enterprise level. This program is based on vulnerability scoring from NIST's National Vulnerability Database with the objective to reduce enterprise-wide cyber security risks by:

- Measuring risk in multiple areas with flexibility to address evolving risks
- Motivating management and administrators to reduce risk
- Measuring improvement
- Providing a single score for each host and each site
- Providing a single score for the enterprise

While our security scoring solution is not "shrinkwrap-able" as a product, the methodology and approach can be ported to any organization. The methodology is tool agnostic. iPost leverages the following COTS products to execute the scoring criteria and publish the dashboard:

- Microsoft Active Directory
- Microsoft Systems Management Server (SMS) or System Center Configuration Manager (SCCM)
- Tenable Security Center

The risk scoring program at State evolved in three separate stages:

- Deployment of above Enterprise management tools
- Delivery of operational data to the field in an integrated application, iPost
- Establishment of a risk scoring program and updates to iPost

This evolution occurred over several years and each stage was envisioned only after the previous stages were relatively mature. As a result, it is not possible to break the costs out retrospectively.

However, the incremental costs for the risk scoring program are minimal considering that we first deployed these enterprise tools to manage a worldwide network. About five staff-years of effort were invested over a two year period to integrate existing tools to implement the risk scoring solution. Attached is a paper that provides an in-depth discussion of our security scoring methodology.